

LandWarNet 2020 and Beyond: A Network for Today and Tomorrow

By Lt. Gen. Susan S. Lawrence, U.S. Army Chief Information Officer/G-6

The average American household knows what it's like to take a cut in resources. You need to plan ahead, trim expenditures, purchase judiciously and find ways to maximize what you already have.

The Army now finds itself in a similar position. We expect that, for the foreseeable future, there will be less money. Over the next three years, there also will be fewer and fewer people. And, though combat operations overseas may be winding down, the overall threat environment will remain the same: unpredictable, unconventional and unceasing.

Relinquishing the Army's land power dominance is not an option. So, just like any family or business facing diminishing resources, the Army must figure out now how to adapt and how to maximize the effectiveness of the Soldiers, systems and dollars available. A modernized, unified network is central to the solution.

The network already serves as the backbone of today's force. On any given day, nearly everything the Army does is tied to or relies upon the network. It's the primary tool for effective management of the Army's human, financial and materiel resources. It is the means for live, virtual and constructive training. Perhaps most importantly, the network carries the information - data, voice and video -- every Soldier and leader needs to act decisively and effectively, making it the Army's most empowering system in an operational environment.

With the number of uniformed personnel expected to drop by about 15 percent over the next three years, a robust, technologically advanced network will become even more crucial. The American Soldier can never be supplanted. But his or her skills and capabilities can be greatly enhanced with the right technology, keeping a smaller force ready for and effective in all mission scenarios.

The challenge in tapping the network to strengthen the Army is multifaceted: construct and maintain a flexible, adaptable infrastructure that reaches from stateside garrison to the farthest tactical edge; get individual technologies and applications into the hands of the Soldiers and commanders who need it as they become available; ensure interoperability upfront, rather than relying on the user to figure it out; and do it all in a financially prudent manner. The solution is integrated management of the network, from start to finish and from end to end.

Applying a portfolio approach to setting requirements, budgeting, development and acquisition is the first step in integrated management. The Network Mission Area (NMA) provides this framework for three domains: network capacity, enterprise services

and network operations and security – just as the Enterprise Information Environment Mission Area did. However, in addressing these domains, the NMA also looks at the Warfighting and Business Mission Areas to understand the *entire* network – not just the underlying infrastructure but every capability, application and system that will ride the network, from the strategic core to the tactical edge. By broadening the scope, decision makers will understand how choices in one mission area would impact the others and where synchrony is lacking, both from timing and interoperability perspectives. With the NMA, the Army no longer will have capabilities sitting idle because they don't work with the rest of the network or are waiting on delivery of another system in order to become operational. Wasted investment will become a relic of the past, allowing the Army to apply its scarce resources to maximum effect.

The second step in integrated management is placing the institutional side on par with the operational. Over the last decade, the Army has allocated significant resources to transforming the operational components of LandWarNet. A necessity while fighting two wars, the focus on the operational inadvertently led to the atrophy of the network's infrastructure and non-tactical components. While deployable forces and power-projection platforms benefited from big budgets, high bandwidth, cutting-edge capabilities and augmented security, the institutional Army frequently relied on decades-old technology and received inconsistent, unsynchronized funding for network modernization programs.

However, today's changing national security posture and objectives mandate that LandWarNet's institutional components also be transformed. For example, to truly be ready for any mission, the Army must train with and use at home station the same technology and procedures as in theater. Prior to deployment, units must be able to right-seat ride with forces already in the area of operations. And, once in theater, the footprint must be smaller, which means relying more on reaching back to capabilities based elsewhere. These requirements, as well as many others, dictate that the institutional side of the network be as powerful and modern as the operational, with the same or greater bandwidth, a flexible up-to-date infrastructure and the capacity to handle all of the Army's business and warfighting needs.

The Army can't just invest *more* in the network's institutional components; it must invest more and do so *more wisely*. Which leads to the third step in creating a unified network: applying capability set management (CSM) across the board. About two years ago, the Army began using CSM for its operational (tactical) systems. CSM evaluates the current environment, then designs a suite of systems and equipment -- a "capability set" -- to answer the projected requirements of a two-year period. By aligning funding and timelines for all programs in the set, operational units receive an integrated network capability at the right time in the Army Force Generation cycle. All elements of the network are thoroughly tested to ensure individual performance, interoperability and compliance with architectural standards before fielding, then procured and distributed together throughout a combat formation. To keep technology fresh, every 24 months or

so, the Army will distribute the next capability set, which will reflect any changes or advances in technology.

To maximize LandWarNet's efficacy, and realize the full potential of Network Mission Area portfolio management, the Army must expand the capability set approach to include the whole network. Network Capability Sets (NCS) will integrate operational and institutional requirements, synchronizing the hardware, applications and services that support both warfighting and business operations. NCS will be comprised of two pieces: Operational Capability Sets (OCS) that include the Mission Command systems, applications, communications transport and services that support units and organizations while deployed; and Institutional Capability Sets (ICS) that include the hardware, applications, services and communications transport necessary for day-to-day Army business activities, installation management and supporting operational units when they are at home. OCS and ICS will connect via the Army's Fixed Regional Hub Nodes and through certain collaborative systems such as Installation as a Docking Station, which allows units to access coalition networks and gain situational understanding before deployment.

The Chief Information Officer/G-6 will design Network Capability Sets, and G-3/5/7 will select and prioritize the receiving installations and units. The Army intends to field the first complete Network Capability Set (operational and institutional components) in fiscal year 2015.

In the near term, NCS will focus on four areas. The first is capacity. The Army's institutional and operational needs are simply enormous. The entire force must have uniform accessibility, throughput, transmission speed and reliability, no matter the location -- operational theater, home station, Army and Joint training centers, or data repositories. Capacity is the key, and will make or break the network's usefulness as a business tool and force multiplier.

The second is enterprise services. The Army must simplify and extend access to data, applications, collaboration tools, communications and other services, for itself and all authorized partners. Taking an enterprise approach is the most effective way, from both functional and economic perspectives, to assure this critical availability.

The third is network operations and security. If the network goes down, the Soldier on the ground is put in jeopardy and leaders cannot make informed decisions. Every user also must have complete confidence that the information and services he sends and receives over the network have not been compromised by the enemy. NCS will therefore concentrate on expanding visibility of the network (assets and device control), implementing strong defenses against attack and defining defense command-and-control responsibilities, and developing the means to mitigate security breaches if they occur.

The fourth focus area, architectural standards, underpins all the rest. For the network and all technologies riding it to be integrated and reliable, firm architectural standards and conformance to them are mandatory. Standards also will help streamline operation and maintenance, possibly lowering cost, and simplify network defense.

Standardization is essential to laying the foundation of and moving the Army into the Joint Information Environment, as well. There is no doubt that future U.S. military operations will require joint responses; designing the Army's network to be inherently joint is the only responsible way forward.

The American Soldier is irreplaceable and remains the most capable, discriminate weapon system ever fielded. But, as the Chief of Staff, General Ray Odierno, says, behind the Soldier the Army must have the most capable, powerful network ever built. As I sign off after 40 years of service to my country, I believe the Army has a solid plan in hand and is on the path to giving Soldiers the network they need and deserve. I am extremely proud of everything the information technology and Signal communities have achieved so far, and, with the support of the Office of the Secretary of Defense, the Congress and industry, I know we can make the next-generation network a reality. Our Soldiers are counting on us.